Dirk van der Linden*, Matthew Edwards, Irit Hadar, and Anna Zamansky

Pets without PETs: on pet owners' under-estimation of privacy concerns in pet wearables

Abstract: We report on a mixed-method, comparative study investigating whether there is a difference between privacy concerns expressed about pet wearables as opposed to human wearables – and more importantly, *why*. We extracted the privacy concerns found in product reviews (N=8,038) of pet wearables (activity, location, and dual-function trackers), contrasting the (lack of) concerns and misuse to a curated set of reviews for similar human-oriented wearables (N=20,431). Our findings indicate that, while overall very few privacy concerns are expressed in product reviews, for pet wearables they are expressed even less, even though consumers use these devices in a manner which impacts both personal and bystander privacy. An additional survey of pet owners (N=201) eliciting what factors would cause them to not purchase (or stop using) pet wearables indicated comparably few privacy concerns, strengthening the representativeness of our findings. A thematic analysis reveals that the lack of privacy concerns may be explained by, among other factors, emotional drivers to purchase the device, and prioritization of (desired) functionality to support those emotional drivers over privacy requirements. Moreover, we found that pet wearables are used in different ways than originally intended, which raise novel privacy implications to be dealt with. We propose that in order to move towards more privacy-conscious use of pet wearables, a combination of understanding consumer rationale and behavior as well as ensuring data protection legislation is adequate to real-world use is needed.

Keywords: Human factors, usability and user-centered design for PETs; Machine learning and privacy; Mobile devices and privacy

DOI 10.2478/popets-2020-0009
Received 2019-05-31; revised 2019-09-15; accepted 2019-09-16.

1 Introduction

An increasingly prevalent type of wearable is the pet wearable, monitoring e.g., pets' activity, location, and other vital information [39]. The market size for this technology has grown significantly over the last years [22], but surveys of wearable technology and its impact on our lives have paid little to no attention to them (cf. Seneviratne et al. [60]). This is a potentially dangerous oversight. Pet wearables have much of the same functionality as human wearables, are regularly deployed in as revealing a manner, and have the same potential technical vulnerabilities. It is already the case that consumers are often left unaware of data collected by apps running on their own phones [6] – consider what privacy implications are going unexamined when those apps are purportedly monitoring pets, rather than the consumers themselves. This represents a particularly important case to study, because while pet wearables may on a first glance seem to be 'for' pets, they capture more owner data than expected [68], impacting their privacy, even though they may remain unaware of this.

To address this, we conducted a mixed-method, comparative study between reviews of pet-worn and human-worn wearables. We investigate whether there is a distinct level of privacy concern expressed by consumers of each technology, and qualitatively investigate review semantics in detail to understand *why* such distinctions may arise. We use a corpus linguistics approach to identify reviews with privacy concerns, following this with a qualitative thematic analysis that explores the following research questions:

RQ1. Is there a difference between privacy concerns expressed about pet wearables and those expressed about human wearables?

RQ2. What privacy concerns are expressed about pet wearables?

***Corresponding Author: Dirk van der Linden:** Bristol Cyber Security Group, University of Bristol, E-mail: dirk.vanderlinden@bristol.ac.uk

Matthew Edwards: Bristol Cyber Security Group, University of Bristol, E-mail: matthew.john.edwards@bristol.ac.uk

Irit Hadar, Anna Zamansky: Department of Information Systems, University of Haifa, E-mail: {hadari,annazam}@is.haifa.ac.il

RQ3. What explanations underlie the extent and type of privacy concerns expressed about pet wearables?

The contribution of our work includes:

We provide a data-driven study of wearable reviews, highlighting consumers' (lack of) privacy concerns for pet and human wearables. Pet wearable reviews express relatively fewer privacy concerns than similar human wearables, by a factor of 2.3. Moreover, taken in absolute terms, reviews express so little visible privacy concern that prospective customers are not likely to be exposed to the potential privacy risks associated with these devices when shopping online.

We discuss the role that emotion plays in trumping privacy concerns, and how marketing of pet wearables plays into such emotions to effectively preempt privacy considerations. A major motivator for the purchase and use of pet wearables is grounded in avoiding negative emotional experiences – when a pet goes missing, or when it is unintentionally given poor care. This places pet wearables in a context being perceived of as fundamental to avoid repeating negative emotional experiences, which may overpower any other concern – whether towards privacy, aesthetics, or even functionality.

We provide insight into the use of wearables outside their original scope and its impact on privacy threats. Pet wearables are at times used to monitor humans, adult and child alike, regardless of manufacturers' attempt to prevent so. As a result, data leaks may be of higher risk than originally envisioned. Consumers will continue to use devices outside of the scope for which they were designed. We thus argue this concern could be most realistically, and effectively, mitigated by ensuring data protection policy that stimulates data security measures, to account for worst possible scenarios, rather than 'reasonable' or 'appropriate' measures to the originally envisioned risk.

2 Related work

2.1 Pet wearables and privacy concerns

Pet wearables are similar in function to most human wearables, consisting of a physically worn device and accompanying software usually installed on the user's phone or accessed via the web. There is one key difference: the physical device is worn by the pet.

A review of the privacy policies of commercially available pet wearables [68] has shown there is a critical mismatch between how these devices are marketed and their transparency in what data they captured. Six devices with activity tracking functionality did not detail any pet activity data in their privacy policies, while seven devices with location tracking functionality did not detail any location data in their privacy policy. Moreover, most devices capture more owner data than pet data, and remain unclear about what pet activity data is actually stored. While there is relatively little extant research on privacy of pet wearables, it is a topic of growing public interest. Mozilla's "*privacy not included" [46] project has a Pet category, with privacy concerns discussed for several common devices like Whistle and Tractive, and even non-wearable smart devices such as automatic feeders and pet cameras. Moreover, technical investigations into dataleaks among pet wearables have been reported focusing on Bluetooth Low Energy (BLE) weaknesses, demonstrating the viability of Man-in-the-Middle attacks and data interception [67]. In a study of service dog training, Zamansky and van der Linden [76] found that guide puppy dog raisers were divided on the question of whether dog activity data from such trackers constitutes personal data capable of identifying them (hint: it does), finding an even 3-way split between those who thought it did, those who thought it didn't, and those who had no idea. Perhaps more importantly, the study found that while raisers of puppies were fine with sharing such potentially personal data with the guide center for which they raised these puppies, the management of the center was far less willing to officially use such wearables for the privacy implications they would hold in terms of capturing indirect information of the puppy raisers. Motti and Caine [45] presented a taxonomy of privacy concerns held by users of commercially available wearables, importantly noting that these concerns are "not necessarily unique to one specific device or form factor, but are intimately related to the sensors embedded in the device." The eleven concerns, grouped under *sensors, data,* or *device and application* specific privacy concerns are listed in Table 1.

Spiller et al. [63] investigated whether, and how users of Quantified Self (QS) technology value privacy, finding that beyond its immediate use to themselves (e.g., informing their own activity) users perceive it to hold little value and subsequently hold little privacy concern about how manufacturers or even law enforcement would use such data. In stark contrast, an overview of the state of security and risks in quantified

Table 1. Taxonomy of privacy concerns and explanation [45] with examples.

concern	explanation	example of threat
access_control	that organizations or government agencies will use their personal data without their awareness or consent	Data collection such as the Cambridge Analytica data breach involving 50 million Facebook profiles
location_disclosure	that malicious parties may track their location and misuse knowledge of their physical whereabouts	Use by stalkers to track someone
social_implications	that unaware third parties may be sur– or sous-veilled by devices without their approval	Impacted bystander privacy in public space due to the proliferation of IoT devices
users_fears	that certain data types when combined could have critical implications	Fitness tracker activity data combined with personal identification data being sold to insurance agents, leading to higher insurance premiums
right_to_forget	that data will be preserved that the users would prefer not to capture or be reminded of	Embarrassing or compromising photos on social media that impact on e.g., job or study chances
surrep_recording	that non-obvious sensors present opportunities for misuse or privacy invasion	Google Glass style concerns
criminal_abuse	that personal data may facilitate criminal acts	several of the above, depending on extant legislation
social_media_sync	that technology may automatically broadcast their activity on social media, without any user control	unaware 'check-in' of location on social media networks

self technology by Barcenta et al. [9] discussed several risks borne out of this kind of data, including identity theft, profiling, location stalking, embarrassment or extortion, and corporate misuse. They concluded that the state of security in self-tracking technology is severely lacking; apps and services are provided without privacy policies or basics such as secure handling of usernames and passwords. Similarly, Leibenger et al. [40] found that privacy policies of QS service providers allow usage of data for diverse purposes by third parties, likely in contrast to what users would be comfortable with. A large-scale study of internet users on disclosure concerns showed that (personal) exercise patterns were one of the least upsetting data types, while compromising media and financial authentication data ranked highest [38]. Such concerns are grounded in concrete vulnerabilities of existing wearables, as shown in an extensive survey of consumer wearables [60] spanning from typical activity trackers to smart textile implants – albeit ignoring pet wearables or indeed any wearable not directly worn by a human. A systematization of knowledge on privacy on mobile devices by Spensky et al. [62] found that many privacy related vulnerabilities arise due to the complexity of software ecosystems, as technologies to protect privacy tend to focus on small parts of the ecosystem, abstracting away from its entire complexity.

Pu and Grossklags [54] investigated factors that influenced users' privacy concerns towards data of themselves and data of friends (e.g., through Facebook connections). They found that past negative experiences with privacy invasions were negatively associated with trust of third-party app handling of personal data. Coopamootoo et al. [19] investigated differences between privacy attitude and sharing attitude, showing that privacy attitudes were more strongly correlated with expressed emotions and relations to others, concluding that privacy attitude and sharing attitude can be classified with good discrimination.'

Potentially relevant to the way dogs in public space are likely perceived as innocuous (from a privacy perspective), Wang et al. [70] showed that privacy concerns regarding drone usage particularly highlight powerful yet inconspicuous data collection, as well as hidden and inaccessible drone controllers, rendering their existing privacy practices futile. Similar to drones, dogs in public space whose location is tracked could also have significant privacy implications. Field studies examining the public use of smart glasses revealed that bystanders expressed interest in being asked permission before being recorded, as well as desiring technology to block being recorded [23]. Ağır et al. [5] discussed the threat of location data being linked with its semantics as a way of learning about people's behavior (e.g., people go to cinemas after going to restaurants), experimentally showing significant risk for users' semantic location privacy.

2.2 Understanding consumers through review analysis

Analysis of online customer reviews has been used in an increasing amount of research. Perceived review helpfulness has been found to be correlated primarily with extremity, depth, and the type of product reviewed [47]. Trenz and Berger [65] found research primarily using reviews to investigate effect on sales, bias and fraud,

review helpfulness, and, particularly relevant, research which analyzes online reviews to extract quality dimensions important to customers (i.e., what they are concerned about). For example, Nelson [50] who investigated parental anxiety as reflected in online customer reviews on Epinions.com. Researchers have conducted content analyses to extract quality dimensions, proposing frameworks to assess online service quality incorporating review data [74], as well as directly investigating quality dimensions relevant to hotels [16], brokerage services [73] , and even concerns about medication information [32]. Amazon is the most popular source of online reviews for researchers [65], primarily because of the extensive number of reviews, as well as lack of censorship. Amazon consumer reviews have been used by researchers to understand the positive and negative elements of consumer technology. Jack and Tsai [34] compared the text of a total of 19,080 reviews related to 40 laptop and tablet devices, identifying the importance of features such as battery life and touchscreen display in relation to the product price. Amazon reviews have also previously been explored to understand consumer safety issues. Winkler et al. [72] built and validated a keyword-based scoring system for identifying reviews containing toy safety concerns, and Bleaney et al. [12] built textual classifiers to identify safety issues in baby products, using a list of recalled products to develop a labelled dataset wherein 424 of 2,285 reviews mentioned product safety issues.

3 Method

3.1 Ethical consideration

We obtained approval from our Institutional Review Board (IRB) before any empirical work began. We did not extract any personal information from reviews (e.g., usernames), although some reviewers provided potentially self-identifying information in the body of their review such as email addresses. We identified reviews by a unique anonymous identifier for reviews of human wearables (Hn) and pet wearables (Pn).

3.2 Model & research variables

Figure 1 (see Appendix C) shows the key entities we study. Each box represents one of the key concepts – wearables, reviews, privacy concerns, and the way in which they relate to each other (e.g., wearables have reviews, which may contain privacy concerns). We hypothesized that pet wearables will be correlated with less privacy concerns compared to human wearables; pure activity type devices will be correlated with less privacy concerns than other devices for both audiences.

3.3 Materials

Table 2 shows the devices included along three main identified categories: pure location trackers, pure activity trackers, and combined activity and location trackers. The n for pet wearable reviews is lower due to 'human' wearables' more widespread use. Quantitative comparisons have been appropriately normalized to account for this difference in numbers.

3.4 Procedure

Figure 2 (Appendix C) shows the process flow of our study. We crawled for English-language reviews of pet wearables posted on amazon.[com/ca/co.uk], using the Amazon 'Pet Tracker' category and a list of devices from a comparison of pet wearables' privacy policies [68]. Excluding devices with < 20 reviews at the time of writing, we then matched the results with similar human wearables. Review text and metadata was then extracted for all devices.

To identify terms used in relation to wearable privacy, we constructed a set of keywords based on Motti and Caine [45]'s analysis of privacy concern in wearable devices. Using the review fragments coded by Motti and Caine as a corpus of privacy-concern-focused wearable review language, and using the human wearable reviews as a topic-matched non-privacy-focused corpus, we performed a keyness analysis using standard statistics from corpus linguistics. We calculated keyness for all words present in both corpora. For $i \in 1, 2$ referring to the two corpora, with O_i being the *observed* count of instances of a word in the corpus, and N_i being the total corpus size in words (less O_i), first an *expected* total E_i is calculated

$$E_i = \frac{N_i \sum_i O_i}{\sum_i N_i}$$

After which the *log-likelihood* [57] can be calculated for the given word as

$$-2ln\lambda = 2 \sum_i O_i ln(\frac{O_i}{E_i})$$

Table 2. Overview of selected wearables and data.

Producer	*Device*	n	★
PET WEARABLES		**8038**	**3.6**
Location trackers			
Loc8Tor/TabCat	Loc8Tor/TabCat	612	3.6
Tractive	Tractive	188	3.7
Eureka Technology	MARCOPOLO	65	4.1
Pet Access 88	Unbranded	30	2
Tractive	TractiveGPS	815	3.5
Activity trackers			
Poof	Poof Bean	41	3.7
FitBark	FitBark	319	4.2
Tractive	TractiveMOTION	22	3
Poof	Poof Pea	50	3.5
Activity & Location trackers			
Findster	Findster Duo+	38	4.3
DOTT	DOTT	80	3.3
Link AKC	Link AKC	748	3.5
Whistle	Whistle 3	3,737	4.4
Whistle	Tagg	1,293	3.5
HUMAN WEARABLES		**20431**	**3.8**
Location trackers			
Spy Tec	STI GL300	3,068	4.2
Aware GPS	ATAS1	55	4.3
Amcrest	AM-GL300 V3	132	4
OLTEC	Unbranded	136	3.2
Tile	Tile Sport	1,321	3.7
Activity trackers			
FitBit	FitBit Alta HR	4,066	4
LETSCOM	Unbranded	278	4.5
Garmin	Garmin vivofit	4,667	3.8
LinTelek	Unbranded	307	4
Activity & Location trackers			
FitBit	FitBit Charge	714	3.5
Huawei	Huawei Band 2	312	3.5
Samsung	Samsung Gear Fit 2	3,220	3.3
TomTom	Runner GPS Watch	969	3.8
Moov	MOOV NOW	1,186	3.9

This is also known as the G^2 statistic. We used a standard significance cutoff of $G^2 > 6.63$ (equivalent to $\alpha < 0.01$) to filter keywords. To enable analysis of the resultant keywords, we sorted them by their *log-ratio* [29], an effect size metric, rather than G^2, following developing best practice in corpus linguistics [25].

$$F_i = \frac{O_i}{O_i + N_i}$$

$$LR = log_2 \frac{F_1}{F_2}$$

We also discarded keywords with $LR < 1$, to focus on terms strongly associated with the privacy concern corpus rather than the general review corpus. We then manually assessed the keywords in context through concordancing, and the keyword list was refined and extended through an iterative search and review phase, with reference to the concern descriptions used by Motti and Caine [45]. In matching, keywords and review text were stemmed using the Porter stemming algorithm [53] to allow for pluralised or tense variants of the keyword form. To reduce false-positives in keyword matching, a word-sense filter was also applied. We assigned search keywords appropriate senses manually through dictionary review, and the senses of textual matches in reviews were automatically derived using the WordNet adaptation of the Lesk algorithm [8], using the review context and derived part-of-speech tag.

A selection of the resulting (78-item) keyword list, after refinement, is shown in Table 5 (Appendix C), sorted by the normalized odds of hits in the pet and human corpora. Reviews which matched at least two keywords were selected for manual review and analysis – to identify if a true privacy concern had been identified, and as input for the thematic analysis. The word 'privacy' was rarely used to discuss actual privacy concerns – likely because consumers describe the concerns themselves, or indirectly approach such concerns.

The manual coding of reviews to identify true privacy concerns was done by one author and verified in a random 10% sample by another author (Cohen's $\kappa = 1$ for pet, .95 for human). High agreement rates are likely due to very low rates of privacy concerns, and clear-cut other focus of reviews. Where significant interpretation of review text was needed to identify a privacy concern we excluded them. For example, negative sentiment such as "I bought the system to track my dogs not share their activities on social media" may be due to an underlying privacy concern, but could equally be because of simple functional requirements, and so would be excluded.

In parallel to the coding of reviews and the quantitative analysis, we performed a qualitative analysis – thematic analysis following Braun and Clarke's method [15] to be specific – on the set of reviews selected for manual review (962 for pet, 1299 for human) to systematically detail what explanations underlie the extent and type of privacy concerns expressed in the reviews. Two authors independently familiarized themselves with these datasets and generated a list of codes, which were consolidated into a codebook detailing the most salient themes [15]. We focused on identifying themes relevant to privacy, especially noting reasons for why people purchased pet wearables, and sometimes unexpected ways in which they use them.

3.5 Limitations

This study only investigated a limited number of wearable devices compared to the large numbers of wearables on the market. Similarly, the investigated review count was comparatively low at $n = 28,469$ to allow for detailed and qualitative analysis following initial classification. To ensure that our sample did not over or under-express the extent of privacy concerns, we used a purposive sampling strategy to extract reviews from Amazon. Because privacy concerns may differ depending on sensors contained in a wearable [45], we first built a balanced set of pet wearables by selecting three subsets: devices which only track location, devices which only track activity, and devices which track both. We constructed a matched set of human wearables following similar distribution, also accounting for known/unbranded devices, and price class. We built our classifier based on the coded corpus used by Motti and Caine to identify a taxonomy of privacy concerns [45], to ensure that the keyness analysis used as input for the review extraction was based on validated data showing privacy concerns.

Our analysis focuses on English-language Amazon sites. Thus, these results may not be representative for all pet owners, as some cultural backgrounds with different attitudes towards privacy may be under-expressed. However, we cannot accurately claim that these reviews represent solely pet owners from Anglo-Saxon cultures either, as people may purchase devices on Amazon sites outside of their own countries, and subsequently leave reviews in English. Fake reviews, while a concern for some studies, tend to affect samples by introducing positive, high-scoring reviews in order to increase visibility of a product and aid in its popularity (cf. Mukherjee et al. [48] for an overview of the rise of 'opinion spammers' and the business of paying for positive reviews). Given that we are focused on finding negative reviews, we did not need to take additional steps to detect or rule out potential fake reviews not already deleted by Amazon.

4 Quantitative analysis

We calculate the absolute and relative proportions of review corpora identified as containing privacy concerns, examine the visibility of these concerns to the public, and compare devices which are more positively or negatively rated by reviewers.

4.1 Reviews with privacy concerns

Following manual coding to confirm reviews containing privacy concerns, we identified 5 reviews in the pet wearable corpus, and 29 reviews in the human wearable corpus. Normalised, this equates to 0.06% and 0.14% of the overall review corpora which raise privacy concerns. Even if we were to consider the keyword-selected manual review set as nothing more than a random sample – a pessimistic upper bound – this estimates 0.52% of pet reviews and 2.23% of the human reviews would contain privacy concerns. We can say that *very few wearable reviews express privacy concerns.*

Despite our keyword filter producing relatively more hits within the pet review corpus, at a normalised ratio of 1.88 pet:human, the results from manual coding demonstrate a strong bias in the other direction (2.28 human:pet overall, 4.3 human:pet within the reviews manually coded). A χ^2-test ($\alpha = 0.05$) shows a significant difference in the proportion of reviews addressing privacy concerns between the manually reviewed pet and human corpora. The indication is that *reviews of human wearables are significantly more likely to include privacy concerns than are reviews of pet wearables.*

Further coding of these reviews with the Motti taxonomy identified a slightly higher number of specific concerns, summarized in Table 3. Access control, location disclosure, and (unwanted) social media sync represent the majority of identified privacy concerns, with access control – a fear and distrust of providing companies with data gathered by devices – being a clear primary concern. The different normalized ratio of privacy concerns between pet and human wearables is in line with the expected relationships from Fig. 1 – although we do not claim to make judgments due to the small sample size. Nonetheless, these numbers may indicate the existence of factors further reducing the already low likelihood of consumers identifying privacy concerns for wearables when these devices are intended for pet use.

4.2 Visibility of privacy concerns

Amazon reviews are ranked by "helpfulness", as voted by prospective buyers considering a product. We examine the mean helpfulness of reviews with privacy concerns, to understand if these concerns are likely to be reaching the public. This consideration is important – if only a small proportion of reviews mention privacy concerns, but these reviews are all highly-rated, it would demonstrate a somewhat wider public awareness

Table 3. Number of identified reviews with (specific) privacy concerns for pet and human wearables. All reviews were written by different reviewers. Normalized where $\neq 0$. Normalized ratio of identified privacy concerns human:pet ≈ 2.3

concern	pet n (normalized)	human n (normalized)
access_control	3 (.04%)	18 (.09%)
location_disclosure	1 (.01%)	8 (.04%)
social_implications	0	1
users_fears	0	1
right_to_forget	1 (.01%)	0
surr_av_recording	0	0
criminal_abuse	0	0
social_media_sync	0	4 (.02%)
other	2 (.02%)	2 (.01%)
Σ concerns	7 (.09%)	32 (.16%)
n reviews	5 (.06%)	29 (.14%)

of these concerns. The mean helpfulness of all pet wearable reviews was 3.52 (median: 1), while the mean helpfulness of the subset identified as containing privacy concerns was 2.6 (median: 3). This indicates a lower than average visibility of privacy concerns, though a strong conclusion cannot be drawn due to the small size of the subset. The mean helpfulness of all human wearable reviews was 2.96 (median: 0), while the mean helpfulness of the privacy-concern subset was 39.41 (median: 2). This marked difference is largely due to the presence in the subset of a single highly-rated review, which has 1062 positive votes. If this observation were excluded, the mean helpfulness would be 2.89, just lower than the class mean helpfulness. As an additional measure of the prominence of privacy concerns, we calculated the proportion of the text (by wordcount of related sentences) relating to privacy concern in the body of those few reviews which contained any. An average of 29% of text in the pet wearable reviews and 39% of text in the human wearable reviews (this difference is not significant at $\alpha = 0.05$) related to the privacy concerns. A total of 10 reviews (1 pet, 9 human) were mostly ($> 50\%$) focused on privacy concerns. The highly-rated review mentioned above was not one of these 9, with 34% of its text relating to privacy concerns.

The indication is that, *some privacy concerns are also more visible to consumers in reviews of human wearables than in pet wearables* – though the evidence for this conclusion is not strong, as a result of the overall low incidence.

4.3 Comparison of pet wearables by reviewer opinion

A secondary analysis is to examine whether user opinion of pet wearables correlates at all with their (lack of) known vulnerabilities. Even though privacy concerns are rarely mentioned in reviews, it could well be the case that this is a hidden factor driving overall opinion, or correlated with other markers of a well-liked product. This is also an instrumentally useful question – *Does a user who is 'following the crowd' end up with a good privacy outcome?*

To explore this question, we coded reviews for compound sentiment valency using the VADER [33] sentiment analysis system. We then carried out two-tailed Bonferroni-corrected Z-tests ($\alpha = 0.05$) on pet device review sentiment, grouped at the device level, to identify devices with significantly lower or higher than average sentiment. As summarised in Table 6 (Appendix C), the devices found to be significantly more positively reviewed than average were the Whistle 3 and FitBark, while significantly more negative than average sentiment was found for the TractiveGPS, TractiveMotion, Access 88, TabCat, and Tagg devices. We confirmed this result via a second set of corrected Z-tests using star-rating data rather than sentiment inferred from the text of the review, in which the Link AKC and DOTT devices were also found to be significantly more negatively-ranked than average. With the exception of TractiveMOTION, these devices all included location tracking capabilities. Location tracking is perhaps one of the most obvious privacy concerns, and seeing both positively- and negatively-rated devices with this functionality suggests there is no strong relationship between functionality class and user opinion. At a technical level, the Whistle 3, Link AKC and Tractive GPS all contain known vulnerabilities according to [67]. There are no listed CVEs for the other devices, but this may simply reflect a lack of any technical security review of those products. The spread of what little evidence is available suggests no relationship between technical security and public opinion. Of these devices, previous analyses of privacy policies by [68] showed that the Whistle and FitBark were less likely to have mismatches between their stated policy and actual device capability, whereas amongst the negatively reviewed devices also covered, the policies of the Link AKC, TabCat, TractiveGPS and TractiveMotion all had missing information about data the devices were collecting. This is suggestive of a potential relationship between the clarity or completeness of privacy policies and user opinion,

although the small number of devices covered here does not allow for strong claims.

4.4 Comparison to pet owners not using pet wearables

The quantitative analysis in this paper focuses on consumers who have already 'bought-in' to pet wearables. It may be the case that the lack of privacy concerns we identified in reviews is indicative rather of a survivor bias where only those pet owners who hold little to no privacy concerns are willing to buy and use these devices. To mitigate this threat, we performed an additional study with 201 pet owners, asking them what, if any, reasons would make them *not purchase* (or *stop using*) a pet wearable. We presented participants with a number of reasons derived from requirements found in other work with pet wearable users [75] and asked them to elaborate on their choice(s). See Appendix A for the used questionnaire.

We recruited participants through Prolific [1]—a platform for recruiting participants for research, similar in approach to Amazon's Mechanical Turk. Participants' median age was 28 years (±10), 58% were male, 43% female. Of those surveyed, 185 (92%) have not owned or used a pet wearable, although 98 (49%) had heard of them. Sixteen (8%) participants currently owned a pet wearable. Table 4 shows the distribution of all concerns selected by participants. Note that participants could select more than one concern.

Table 4. Pet owners' reasons to not purchase (or no longer use) pet wearables (n=201), distinguished between non-users (n=185) and users (n=16). Privacy represents 7% of overall participants' concerns, not statistically differing between non-users and users.

reason	non-users n (normalized)	users n (normalized)
Durability	86 (46%)	5 (31%)
Cost	75 (41%)	–
Usefulness	43 (23%)	5 (31%)
Welfare	41 (22%)	8 (50%)
Accuracy	37 (20%)	0
Battery	28 (15%)	2 (13%)
Privacy	14 (7%)	1 (6%)
Other	7 (4%)	0

In the small group of users of pet wearables, only one participant (6%) noted they would consider to stop using their pet wearable because of privacy concerns: "I'm afraid of my privacy – e.g. tracking data could leak from operator database and someone would use it against me." In the larger group of non-users, privacy concerns were selected 29 times (16%). We then performed a closed coding of participants' elicited rationale to confirm their reasoning indeed indicated a privacy concern (done independently by three authors, with the resulting coding having an average pairwise Cohen's κ=0.86 and overall Fleiss'κ=0.861, indicating a very good level of inter-rater reliability). This resulted in 14 (7%) of participants expressing a validated privacy concern. This lower number may be explained because the majority of privacy concerns expressed by non-users were expressed as part of multiple concerns (median=2, std=1.3, max=6), and their rationale was less indicative of privacy being a reason to not purchase a pet wearable. Indeed, only 3 non-users (1.6%) noted privacy as the main reason to not purchase a pet wearable.

The proportion of privacy concern does not seem to differ between non-users and users. We cannot find support for either privacy concerns being significantly more expressed among those not using pet wearables, nor that it is more important of a reason to not purchase a pet wearable than others – as Table 4 shows nearly all other reasons outrank privacy concerns. Moreover, if pre-existing concerns would have a significant negative effect on the willingness to purchase of pet wearables, it stands to reason that those concerns should also appear less in reviews of people who did purchase these devices. This can be trivially shown not to be the case for top concerns such as durability, with many reviews talking about pets breaking these devices. Thus, it seems warranted to assume that survivor bias, in the sense of these concerns *a priori* stopping consumers from purchasing them, is not a significant threat to validity. One might explain the lack of *a priori* privacy concerns in terms of research showing that limited technical understanding of devices leads to gaps in consumers' threat models [78], or that consumers willingly purchase such devices, and through the well known psychological process of cognitive dissonance [24] subsequently rationalize that act of purchasing by revisiting their beliefs to solve this contradiction.

However, earlier research has shown that there is little to no relation between self-reported privacy attitudes and behavior, concluding it is simply not possible to infer causal relation between higher general privacy concern [2]. Becker provides an explanation in the context of health wearables for the absence of such a relationship – the dilemma of forced acceptance – that desire for, and subsequent reliance upon functionality overrules such a priori concerns [10, 11].

5 Thematic analysis

We performed a thematic analysis according to Braun and Clarke's established method [15] on the reviews selected for manual review and analysis – 962 in the pet set and 1299 in the human set. Thematic analysis is a systematic approach to identify and examine reocurring meaningful themes in data. In this particular case, our analysis focused on systematically identifying what explanations underlay the (lack of) privacy concerns expressed in this set of reviews. A codebook was established by two authors, shown in Appendix B.

This analysis led to a more nuanced view of the lack of privacy concerns, indicating that there are various factors that trump consumer's own privacy concerns, as well as their privacy concerns towards bystanders. On a high level, we divided these into themes characterized by one of the following (1) Privacy concerns being trumped by another factor, (2) bystander privacy concerns being trumped by another factor, and (3) pet wearables worn by humans. The below sections will detail the identified individual themes identified which provide explanations that underlie the lack of privacy concerns expressed across these three major themes.

5.1 Privacy concern is trumped by another factor

Only 0.06% and 0.14% of reviews on pet and human wearables respectively mentioned privacy concerns – most of them as a sideline. An intuitive conclusion to draw would be that consumers do not care about privacy, certainly in line with other research [3, 37, 63], and perhaps most easily observed by how widespread the "I've got Nothing to Hide" sentiment is [59], even though it "represents a singular and narrow way of conceiving privacy" [61].

. . . because functionality trumps privacy?

Just as in the development of technology (cf. [18]), functional requirements and concerns typically trump consideration of any other requirements, certainly privacy. Take, for example, a review which argues for the inclusion of usable social network functionality in a pet wearable's app:

> "The app lacks a good social component, so it's hard to meet other fitbark dogs and make friends with them - you have to know the other dogs email address to compete with them which is a bummer. I just want to know who has fitbark nearby so I can friend, compete and socialize with them." **(P2725)**

While the functionality is there – emailing other people to add them as friends, it is not perceived as simple. Rather, this reviewer just wants it to work, by the app allowing them to see all other devices nearby them, and allowing them to send friend requests. However, to do so, at the very least continuous location permissions would have to be granted to the app – something likely perceived as invasive by consumers [27], as well as making all data collected more sensitive by having it linked to detailed location patterns.

Another reviewer expressed their desire for functionality that would arguably bring them closer to their dog by enabling direct communication and awareness of their physical context:

> "Only thing that would make this better is if the beeper was actually a speaker and camera so you could talk to your dog and get photos of what he sees. I am looking forward to an enhancement of this nature." **(P1154)**

There have been (attempted) pet wearables incorporating audio and video sensors. For example, WÜF, claimed to be the world's "smartest dog collar", incorporated a microphone and speaker to allow for bark analysis as well as communication with one's dog (or whatever species wears the device). Their Kickstarter page has been all but abandoned, and their company website [26] is now offline. Perhaps the companies attempting to implement this functionality which consumers desire, ran into the reality of sensors capturing rich data in public leading to more privacy concerns to do with the inability to gather consent from bystanders. Compare also a smart vest for dogs developed in Thailand, intended to reduce animal cruelty by having a videocamera recording whatever the dog sees when it barks [35]. While a noble goal in itself, the premise of video-camera wielding dogs acting as a living CCTV network would certainly lead to equal privacy concerns in areas with stricter privacy legislation.

Similarly, one reviewer expressed their annoyance at their pet wearable not capturing and relaying continuous precise location.

> "I don't know why their tracker can't be real time since it tracks my phone real time."**(P6979)**

Perhaps as a result of the functionality provided by real-time tracking of their phone location, they equally ex-

pect this functionality of other devices, no longer affording an initial consideration of whether such functionality has other implications.

Another functionality appreciated by several reviewers is the ability of some pet wearables to store veterinarian (medical) records directly on the wearable. These records are necessary for veterinary care, and may also be required for things like pet daycare to prove vaccination status, and so on. As one reviewer noted, the ability to cut down on documents to carry around is much welcomed:

> "Another cool thing about the app is storing medical records. Since we are new to town I have to re-enroll her in a daycare, dog parks, etc. and I'm so glad I don't have to cart all those papers around with me. I already have enough in my purse!" **(P468)**

Yet, as useful as this functionality is for consumers, it should not be understated that these are *medical records* – even if 'only' of a dog. They contain sensitive information, health status, vaccination status, medical history, all of which may reveal information about the owner and the care they are (capable of) providing. This is not only interesting for pet health insurance companies, but may equally be interesting to their owners' insurance companies, as depending on the wealth of the data – activity and exercise levels, for example, there may be correlations between a dog's health and an owner's health [51].

The sole reviewer expressing discomfort with the storage of veterinary records did so only from a point of view of the functionality not being all that necessary rather than whether it poses a potential threat to their privacy:

> "Vet record recording is neat, but I think it's a little outside of the scope of the use of this collar" **(P858)**

. . . because emotional attachment trumps privacy?

Many reviewers detailed the reasons for purchasing a pet wearable, often rationalizing from an emotional perspective. Prior experiences with losing their pets (the loss [44] and potential death [4, 66] of pets is known to be associated with significant grief and stress) are described as having such a strong emotional impact justifying the need for a pet wearable to prevent such loss, with no other considerations discussed.

For example, one reviewer mentioned having purchased a GPS-enabled location tracker for their dog because a traumatic prior experience of losing their dog:

> "He was missing for 24 hours in a 200 acre natures preserve and *it was the worst 24 hours ever*. As I walked through the woods and fields, I swore when we found him, he was getting a GPS collar so we would never lose him again." **(P5366)** (emphasis added)

Many other reviewers shared similar stories, all with the same underlying theme that the pet wearable has become an essential device to stave off the emotional whirlwind of losing their loved ones:

> "We've spent many nights bushwhacking for lost Airedales, Scotties and Irish Terriers in our last 25 years, had our stomachs eaten away by worry acid, and are on a first-name basis with our local police department. Not any more. *This is one product that we find essential.* " **(P7492)** (emphasis added); "we thought we had lost our dog. My wife was crying and I was at my wits ends. [...] *We could not live through that feeling again*, so we found Tagg Tracker." **(P5357)** (emphasis added)

Additionally, activity trackers lead to an emotional component in consumers' reasoning, as levels of fitness and activity instill a sense of guilt into pet owners on their perceived caregiving:

> "I think seeing their actual activity level will either guilt me into getting busy with them or make me proud of how we're doing." **(P2900)**

This may be linked directly to a pet owners' own health as well, as in the case of service dogs, where the owner's ability to provide good care for the dog indirectly impacts their own health:

> "Having a medical service dog I am always looking for ways to improve and maintain his health, because his health has a direct impact on my own personal health." **(P5320)**

Given the use of activity trackers to inform pet owners in aspects of caregiving to their pets – primarily centered around exercise and diet[1], pet owners seem to purchase such wearables because of emotional drivers which may trump other considerations.

1 In the UK alone over 50% of dogs are clinically obese [21], making for a clear use case.

. . . because consumers cannot "make the leap"?

The notion that functionality trumps privacy considerations is one interpretation for the lack of privacy concerns. Another interpretation is that consumers do not seem to understand privacy concerns, even when faced with clear situations where data is not kept private, because they are not the subject of that data, and do not seem to make the leap that their data may equally not be kept private. Consider the following review fragment regarding a pet location tracker:

> "The app picked up another pet about 10 houses down in my neighborhood. To verify, I walked down to that yard to verify there was a pet there where the app 'saw' it. [. . .] As you can see, my app picked up a second dog from another neighborhood. While she was still on our back yard, I went around the front of my yard, and could see the dog as in the attached photo. So, apparently your device isn't picking up just one other dog, but apparently any dog that happens to have their device turned on at the same time as mine." **(P135)**

This is an alarming observation (if correct), both from a functional perspective – one cannot easily track their dog if the device tracks other dogs at the same time, but more specifically from the privacy perspective – the app reveals location information of other people's dogs, likely without their explicit knowledge. This particular reviewer only raises the concern from a functional perspective, because it makes it more difficult to find their dog, neither explicitly mentioning whether it is bad that they could find other people's dogs, nor reflecting on whether *their* dog's location would also be visible to others using the app.

. . . because there are generational differences in privacy expectations?

Another potential explanation can be generational differences in attitude towards, and expectation of privacy. The few reviewers who expressed concern about scope of data collection referred explicitly to such generational gaps. See for example the disillusionment expressed by a reviewer on the perceived real purpose of their pet wearable:

> "I'm a fairly savvy old geek and I was ready to ship both the collars back. [. . .] I think it's just too damn fancy and wasn't designed for real people or dogs but designed by some 20 y/o tech wizards that want access to your phone data and location 24/7 so they can spam you advertisements. Time will tell but that's my gut feeling." **(P711)**

Another reviewer similarly expressed his discontent with a human wearable framed in the context of the quantified self zeitgeist:

> "Cannot wait to return this thing. Imo, it's a fad, a gimmick and a product of the need to know everything culture we have today." **(H6630)**

However, the challenge of posing such generational differences to privacy expectations is that, while some differences in attitude have certainly been claimed in literature [58, 77], there is yet too little data on current generations to adequately assess whether it is indeed a key difference between old and young.

5.2 Bystander privacy concern is trumped by another factor

If the above section has made a point that people do not seem to care about their privacy, this section will show that they certainly do not care about the privacy of bystanders.

Bystander privacy is known to be impacted by pet wearables [68]. Human wearables are no different in this regard, and may indeed go further in how grievous the infringement of bystanders' privacy is depending on the sensors contained in a device and the data collection they enable – microphones recording all ambient audio, video recording what people do in public, and so on [17, 31]. We found specific contexts in which users of these wearables impede on bystander privacy.

. . . because we want to keep an eye on those interacting with our loved ones

Many reviewers noted the useful functionality of pet activity trackers to verify that pets were active when they should be. In particular, when left with pet sitters, reviewers mentioned finding it useful to check up on their dogs' activity levels in order to indirectly monitor the pet sitter and make sure they were doing their job:

> "It's also been a great device for keeping dog walkers honest. We had a well liked dog walker in our building we hired. His first walk was for an hour. Thanks to our activity tracker we knew for a fact that this guy walked the dogs for all of 5 minutes over the course of an hour. He walked out of our building and sat somewhere for about 40 minutes and

> then came back. So it's nice to have the peace of mind that nobody is cheating your furry friend on their much needed play time." **(P2689)**

While indirectly tracking a pet sitter in this context is not likely to receive much condemnation as infringing their privacy, the extent to which this is enabled by detailed and precise tracking through the pet wearable has the potential to make consumers uncomfortable as they realize it reflects on their behavior:

> "The GPS tracking is unbelievably accurate. I can see when our dog walker arrives and track where they go. I don't do this all the time (kind of creepy stalker-like)" **(P935)**

. . . because, again, functionality trumps privacy

While tracking pet sitters is a somewhat defensible invasion of bystander privacy, several reviews discussed perceived missing functionality that would clearly breach bystander privacy in much more serious ways ("a camera would be cool on future units", as **P4079** noted). Take, for example, this reviewer expressing again the desire to see and hear where their pet has been:

> "We love the device and have only one other wish, could they make a "Go Pro" camera that also attaches so that we could get a video of where she has been and what she has been up to? I'm sure that will be coming in the next version :)" **(P6898)**

While from a pet owner's perspective this would be construed as functionality that strengthens the human-animal bond [30], including such sensors on wearables which are then inconspicuously carried around in public (certainly in the case of outdoor cats roaming freely) would effectively lead to living surveillance networks. Yet, because of the perceived benefits to the functionality, consumers do not seem to make the additional step to reflect on how others using the same technology could affect them, thereby realizing the potential privacy threats. This can be seen for different functionality as well, such as for example a pet wearable providing exact addresses of where the pet has been. One reviewer noted the usefulness of such information, detailing it provided them information they did not have, but, again, not made the leap to reflect on whether this means that their information would equally so be shared with other users of similar pet wearables:

> "The other thing I found helpful was that when you take your pet to a familiar location outside your house (vet, family, park) the app provides you with the current location and asks if you would like to save this as a stored location. Once saved, the tracker points out that you went to the vet, etc. rather than alerting you continually that your pet is outside the perimeter. We stayed with friends in another state and the app provided me with their exact street address -which I didn't even possess!" **(P3288)**

5.3 Pet wearables are worn by humans

People do not necessarily use wearables with their intended audience. As one review emphatically stated, consumers will use them howsoever they see fit:

> "I firmly believe they should not disable the broad range of possibilities for this device to be used for anything that the consumer desires, especially since there is a service for which you need to purchase." **(P3100)**

A variety of use for pet wearables is expressed in the reviews, from pets, to drones ("I needed something light that [. . .] I could attach to my drone as a backup locator." **P883**), to most importantly, *humans*.

. . . because they work well for the cognitively impaired

Whether for reasons of cost, aesthetics, or functionality, several reviews mentioned using pet wearables with cognitively impaired people – typically loved ones suffering from Dementia or Alzheimer's. For example, a reviewer mentioned the usefulness of a location tracker intended for pets over a dedicated 'dementia tracker':

> "I bought this to try and keep an eye on my mother (who has dementia) and her dog. [. . .] I will also add that this tracker actually worked better for keeping an eye on my mother than the much more expensive 'dementia tracker' I also bought at the same time. [. . .] the live tracking feature on the Tractive was much more useful than that on the dementia tracker. The Tractive unit was also smaller and harder to notice" **(P2128)**

While reviews of human wearables also indicated their use in tracking similarly afflicted loved ones, the reviews of pet wearables used for this purpose explicitly stress their suitability over such devices:

> "My mother has alzheimer's and I've been looking for a device I can attach to her that she can't remove, but will alert me when she leaves her assisted living facility 30 miles away from my home. Therefore, it had to be waterproof for showers, and because I don't want to drive there every day to charge it, must have long battery life." **(P6190)**

. . . because they also work well for kids

Besides tracking the cognitively impaired, several reviewers mentioned using pet wearables to track their children's location. In particular, the tracking functionality is described as positive for both parent and child by affording a level of independence in e.g., play:

> "So we don't actually have this attached to a pet – we put it on a belt for our 6-yr old son to give him the freedom to go outside and play with his friends like it's 1988. Serves a couple of purposes: (1) We know where he is when it's time to go get him and (2) if anything did ever happen (God forbid), we'd find him immediately." **(P3452)**

Yet, these devices are not made for humans. Only one review mentioned this fact – but failed to mention *why* the manufacturer may exclude humans from their use, as for the consumer they are exactly the same:

> "I further tested the Tagg by putting it on the cat collar and securing the collar to my daughter's ankle when we went camping. Now, the Tagg company specifically says it is not to be used on children, but I didn't see the harm. She went all over camp with her friends and I would be notified when she was outside the specified zone and I could view her location any time." **(P2128)**

6 Discussion

6.1 How do the findings answer the research questions?

RQ1. Is there a difference between privacy concerns expressed about pet wearables and those expressed about human wearables?

Our findings indicate that reviews of human wearables are significantly more likely to include privacy concerns than are reviews of pet wearables. Thus, quantitatively, the privacy concerns expressed between pet wearables and human wearables differ.

RQ2. What privacy concerns are expressed about pet wearables?

When privacy concerns *are* expressed about pet wearables, they, in line with human wearables, tend to focus on concerns to do with access control (what is done with the data without the owners' consent or awareness) and location disclosure (that their own location may be tracked through their pet's location). However, given the very limited number of expressed privacy concerns both in the review set and the additional study performed with pet owners not using pet wearables, this should not be taken as a representative description of what pet owners worry about in terms of privacy concerns. Thus, qualitatively, the privacy concerns expressed between pet wearables and human wearables are similar to some extent.

RQ3. What explanations underlie the extent and type of privacy concerns expressed about pet wearables?

The thematic analysis revealed several explanations that underlie the lack of privacy concerns expressed about pet wearables. One explanation that could underlie the lack of privacy concerns is that consumers do not make the leap – between the marketing of these devices emphasizing the pet-focus above all else, it cannot be realistically expected of consumers to make the jump in analyzing the details of privacy policies to see *their* data is captured just as much as their pets. Section 6.2 will explore this in more detail.

However, another explanation, expressed to a far greater extent in thematic analysis, is that different kinds of functionality trump other concerns. The benefits of using pet wearables simply outweigh any potential negatives. This may be because of improved quality-of-life that such functionality is perceived to offer, such as storing medical records in a dog's wearable and not having to worry about losing them, or simply by having a rugged device that allows parents to track their children and not fear it breaking during play. Many of these findings show examples known in other contexts of a trade-off or cost-and-benefit decision being made between the functionality of the device on the one hand, and potential negative impacts such as privacy, on the other hand. Section 6.3 will explore this in detail.

6.2 Why should we not expect consumers to make the leap?

Recent research shows that people with deeper understanding of technical models are known to perceive more privacy threats [36]. Such understanding is not necessarily to be expected in the context of pet wearables, as they are marketed to a wide segment of the consumer market through emotional arguments, and do not presuppose any required technical know-how. This is in line with findings from Zeng et al. [78] who found that consumers perceive only a limited extent of potential privacy concerns in smart homes due to limited technical knowledge [78].

However, a key challenge is that consumers do not seem to be aware of (or care about) the extent of data collected by these devices and their associated apps, nor what implications this may hold for them or others. For example, pet wearables which are not purely focused on location tracking, tend to stress their activity tracking capabilities [68]. As consumers' intuitive understanding of what data is tracked prevents them from reasoning about other kinds of data that may be collected [55], the way these devices are marketed also likely pushes consumers to underestimate the data they collect and its privacy implications. Knowing also that consumers are more comfortable with data being collected in public settings rather than private, and are more likely to consent to data collection if they find that data useful [49], the seemingly accepting attitude of consumers to the data collection of pet wearables in public space may be positively influenced by usefulness of e.g., pet location data in avoiding negative emotional experiences.

Coopamootoo and Groß [19] found in a study of privacy and sharing attitudes that sharing attitude significantly increased the likelihood of happiness and decreased the likelihood of fear, whereas privacy attitude increased the likelihood of fear. Similarly, the fact that these devices bring happiness to their users may thus preclude them from critically engaging with their potential privacy implications. Moreover, it is not only the user's own privacy that is potentially impacted by the use of these pet wearables, as bystander privacy can be impacted through both direct recording, or indirect reflection in the dog's activity data. Users seem to be aware of such potential, noting they can observe third parties such as dog sitters and analyze how the activity patterns of their dog changed when they were with this person. Yet, they do not seem to realize that this extends to anyone interacting with their dog, nor themselves interacting with a different dog. This may be due to the novelty of these devices, and the known major concern of inconspicuous data collection when consumers are not aware of how these devices work (such as studied in drones [70]). Unlike the case of pervasive photography where younger generations have been shown to be aware of potential privacy impacts and devised 'workarounds' to prevent negative impacts [56], it seems that pervasive indirect monitoring such as in the case of pet wearables has not yet reached awareness in a large extent of the population.

This may be further explained by research arguing that people develop subjective theories about online privacy which puts them in a default mode of trust. In this mode, they discount the risk of data disclosures, and perceive fewer risks, further reinforcing their propensity to trust [42]. When consumers effectively hold such a 'truth bias' [14], likely mediated by beliefs that they hold towards the low risk of wearables and such technology in general [20, 71], they are less likely to critically assess how these devices are marketed, or what data is (not) collected – especially because doing so takes significant time and mental effort, for no evident reason.

Takeaway: there are several good reasons *why* consumers should not not be expected to make the leap towards identifying privacy concerns of pet wearables. In particular, they cannot be reasonably expected to understand the technical intricacies of these devices and how they capture data.

6.3 Why do other factors trump privacy concerns?

Even though a desire for privacy seems widespread among all cultures and contexts (cf. [43]), the exact perceptions people hold with regards to privacy are heavily dependent on their culture and personal context [43, 64].

Functionality has been found to overrule privacy concerns in many domains. For example, studies among elderly persons found that mobile safety alarms, even though revealing their location, were perceived to be so beneficial to their personal safety and mobility, that privacy was gladly sacrificed for it [41]. Similarly, in the context of surveillance in public space, privacy loss is often explicitly accepted in cases where it is perceived to reduce threats to personal safety, such as CCTV use in urban transportation [69]. The two themes of functionality, and emotional attachment to pets which we identified in our analysis seem to be in line with these studies' findings – the functionality of a pet wearable, even if potentially leading to a loss of privacy, gives benefits to its owner in the form of e.g., avoiding future negative emotional experiences. As a result, the benefit of the device is greater than the cost it may or may not be perceived to have in terms of personal privacy. For example, one of the major reasons we found *why* consumers seem to not care about privacy concerns was their emotional driver in getting these devices. The use of such devices, whether location tracking allowing for never having to fear losing one's pet again, or activity tracking allowing for feeling one can give better care to their pet, clearly links with feelings of happiness. This is perhaps one of the most important links to the lack of privacy concerns.

The emotional drivers for obtaining pet wearables, which our analysis found to be primarily related to dogs running off or cats hiding too well, can certainly be linked to an increase of criminal behavior. Pet theft is on the rise across most Western countries. For example, the American Kennel Club reported rising numbers of dog theft [7], and cautioned owners to not share details regarding their dogs carelessly. The UK-based charity Blue Cross found via Freedom of Information requests to UK law enforcement that dog thefts in the UK increased from ± 1500 to nearly 1800 from 2013 to 2016 [13]. Given the media exposure given to the phenomenon of pet theft, it is likely that consumers are becoming more motivated to use pet location trackers, suppressing any concern they may have had about privacy. The reality of pet ownership in this context, thus, seems to explain why pet wearable' benefits in preventing such negative consequences outweigh any perceived privacy concerns.

Takeaway: there are several good reasons *why* consumers may not appreciate privacy concerns of pet wearables, or knowingly take them for granted because of other factors. In particular, functionality of these devices brings benefits which outweigh other concerns.

6.4 How can policy and legislation protect consumers ?

The introduction of big data initiatives for pet data such as PetCommunity [52], which aims to build a centralized, global data silo of pet data – linked to human identity (!) – available to veterinarians, pet service providers (e.g., groomers, dog sitters and walkers), medical providers (e.g., pet insurance) and researchers, makes it especially critical to ensure that consumers are *informed* about the potential privacy implications their use of pet wearables (in whatever context) entails. While the promise of improved well-being for our pets is a strong driver for consumers to want to share their data for such purposes – as presented in Section 5.1 – it is important for consumers not to let their love for their pets to blind them to what they actually share – detailed, even if indirect monitoring data about their lives. One may either propose that behavior of users should change, for example through cybersecurity advocacy seeking common ground with consumers and providing practical recommendations [28], or, as we would espouse, the view that a reactionary approach to pet wearables being used for humans is not constructive. Rather, accepting that consumers on the one hand use the devices in unintended contexts, and manufacturers see the value in their data on the other hand, should guide our re-framing of how to ensure they impact minimally upon the privacy of their users as well as bystanders. This will require careful consideration of how data protection legislation actually protects consumers in these cases. As we have shown, pet wearables are used in different ways than originally conceived or indeed intended by their developers, and consumers have strong opinions as to whether they should be able to do so. However, the use of these devices in different ways may have consequences for consumers depending on how well data protection legislation allows for and protects consumers in such misuse. In our analysis we have found at least two such scenarios:

1. the sensitivity of location and activity data varies by species – due to their nature as companion animals, dog location patterns are more likely to reveal their owners' location and behavior [68]
2. unexpected use by consumers of pet wearables for human-worn use means a mismatch between expected sensitivity of location and activity data and actual data sensitivity

The technical measures implemented to ensure data security on a device will vary with the risk perceived or assessed by the manufacturer. A location tracking device intended for a cat might have less stringent encryption of the location data to free up computational resources used for other functionality – based on the assumption that location and movement patterns of a cat are not critically sensitive data. The same device intended for a person would have far more stringent encryption of location data, as it is considered more sensitive.

The latter of these complications may prove critical indeed, given that e.g., the geo-fencing ability of some of these devices may allow for fairly trivial SSID spoofing attack. To keep track of pets, virtual fencing is implemented in some cases by the device checking if it is still in reach of a white list of WiFi networks (i.e., home, the petsitter). The warning that is sent when a pet exceeds this reach can be prevented by spoofing a network which mimicks this information. Should consumers be relying on these devices to keep track of their children – as P2128 has, while noting that "I didn't see the harm", the implications of such attacks are all the more critical. Moreover, as P6000 has noted, some devices do not allow for any tracking while believing it is in reach of a white listed network: "[...] if the collar detects your home WiFi signal, you can't activate any kind of tracking. The collar just thinks your pet is at home, and

that's that." Besides such potential attacks, the availability of detailed location data of children through misuse of these wearables is a clear concern.

How does relevant data legislation deal with such scenarios? Take the EU's General Data Protection Legislation (GDPR). Art. 32 (GDPR), states that "the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security *appropriate to the risk*" (emphasis added). What exactly is appropriate is left open to interpretation here. As a result, manufacturers could claim protection appropriate for the risk of e.g., a cat's location data was implemented and complies with the regulation. However, that disregards entirely the unintended use of consumers who greatly increased the risk by using it with a human. The California Consumer Privacy Act of 2018 (CCPA) states rather differently that "a business ... shall implement and maintain reasonable security procedures and practices *appropriate to the nature of the information*, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." (emphasis added) Here, one could argue whether misuse of a pet wearable for human use is covered for by the act, as it speaks of the nature of information captured by the device, rather than risk of its envisioned use. Given that pet activity data may indirectly reveal human (personal) behavior towards dogs, we could argue that pet wearables already should have security practices appropriate for human personal data.

The Israeli Protection of Privacy Regulations (data security) 5777–2017 (IPPR) seems to take a more specific approach, defining a number of items that constitute personal data (without explicitly using that term), and requiring databases holding them to be subject to a "medium level of security," operationalized via specific requirements. Yet, due to its enumerated list of data rather than defined types of information, pet wearables are left in a void as to what protection should apply.

What is left open is the question of how we define reasonable and appropriate security measures in light of the known misuse of these devices outside of their intended context, as well as the ability of animal activity data to reflect people's interactions with those animals. We propose that reasonable here includes accepting the reality of how devices are used (even if not intended), and ensuring that data protection mechanisms are adequate to the most critical use case (i.e., even cat location trackers should implement data protection to the level of human location data). Yet, for this to become reality, precedent will have to be set through legal cases in order to rule to what extent these devices need to adhere to stricter data protection.

Takeaway: data protection legislation should consider the impact of reasonable alternate use of wearables and enact data protection requirements that deal with all potential use rather than restricting to what was originally conceived by developers.

7 Conclusion

In this paper we investigated the privacy concerns expressed by consumers for pet and human wearables in online reviews. We showed that there is a significant difference between the frequency of privacy concerns expressed in online reviews, with pet wearable reviews expressing privacy concerns significantly less than human wearable reviews. The main privacy concern expressed about pet wearables, in line with human wearables, focused on access control. Singular remaining privacy concerns focused on location disclosure and the right to be forgotten. In this regard, while there was a significant difference in frequency of privacy concerns, the *content* of those concerns does not differ significantly.

The *lack* of privacy concerns expressed about pet wearables can be explained by consumers not reasonably being expected to make the leap, more likely, prioritization of functionality over privacy requirements, as well as emotional drivers to get the device. Moreover, while most reviews showed a lack of concern for personal privacy, concern for bystander privacy was even less observed, with many reviews proposing additional functionality clearly infringing on bystander privacy. In addition, we found that people use devices in different ways than originally intended, such as using animal location trackers for children, elderly, or the impaired, with no indication that they realized any potential privacy implications of this misuse.

We proposed that the misuse of pet wearables for human use needs to be considered by policy makers, as current data protection legislation such as the GDPR, CCPA, IPPR are diverse in the extent to which they can protect consumers and their data in these scenarios.

Acknowledgments.

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

References

[1] Prolific. https://www.prolific.ac, 2019. Online; last accessed 8 May 2019.

[2] A. Acquisti and R. Gross. Imagined communities: Awareness, information sharing, and privacy on the facebook. In *International workshop on privacy enhancing technologies*, pages 36–58. Springer, 2006.

[3] A. Acquisti, L. K. John, and G. Loewenstein. What is privacy worth? *The Journal of Legal Studies*, 42(2): 249–274, 2013. ISSN 00472530, 15375366. URL http://www.jstor.org/stable/10.1086/671754.

[4] J. A. L. Adrian, A. N. Deliramich, and B. C. Frueh. Complicated grief and posttraumatic stress disorder in humans' response to the death of pets/animals. *Bulletin of the Menninger Clinic*, 73(3):176–187, 2009.

[5] B. Ağır, K. Huguenin, U. Hengartner, and J.-P. Hubaux. On the privacy implications of location semantics. *Proceedings on Privacy Enhancing Technologies*, 2016(4):165–183, 2016.

[6] H. Almuhimedi, F. Schaub, N. Sadeh, I. Adjerid, A. Acquisti, J. Gluck, L. F. Cranor, and Y. Agarwal. Your location has been shared 5,398 times!: A field study on mobile app privacy nudging. In *Proceedings of the 33rd annual ACM conference on human factors in computing systems*, pages 787–796. ACM, 2015.

[7] American Kennel Club. Protect Your Pet from Theft. https://www.akc.org/press-center/articles/pet-theft/, 2019. Online; accessed 30 January 2019.

[8] S. Banerjee and T. Pedersen. An adapted lesk algorithm for word sense disambiguation using wordnet. In *International Conference on Intelligent Text Processing and Computational Linguistics*, pages 136–145. Springer, 2002.

[9] M. B. Barcena, C. Wueest, and H. Lau. How safe is your quantified self. *Symantech: Mountain View, CA, USA*, 2014.

[10] M. Becker. Understanding users' health information privacy concerns for health wearables. In *Proceedings of the 51st Hawaii International Conference on System Sciences*. AIS.

[11] M. Becker, C. Matt, T. Widjaja, and T. Hess. Understanding privacy risk perceptions of consumer health wearables – an empirical taxonomy. In *Proceedings of the 38th International Conference on Information Systems*. AIS.

[12] G. Bleaney, M. Kuzyk, J. Man, H. Mayanloo, and H. R. Tizhoosh. Auto-detection of safety issues in baby products. In *International Conference on Industrial, Engineering and Other Applications of Applied Intelligent Systems*, pages 505–516. Springer, 2018.

[13] Blue Cross. Dog theft on rise as charity reveals shock figures of pets taken from their homes. https://www.bluecross.org.uk/dog-theft-rise-charity-reveals-shock-figures-pets-taken-their-homes, 2019. Online; accessed 30 January 2019.

[14] C. F. Bond Jr and B. M. DePaulo. Accuracy of deception judgments. *Personality and social psychology Review*, 10(3): 214–234, 2006.

[15] V. Braun and V. Clarke. Using thematic analysis in psychology. *Qualitative research in psychology*, 3(2):77–101, 2006.

[16] M. S. Chaves, R. Gomes, and C. Pedron. Analysing reviews in the web 2.0: Small and medium hotels in portugal. *Tourism Management*, 33(5):1286–1287, 2012.

[17] S. Chowdhury, M. S. Ferdous, and J. M. Jose. Bystander privacy in lifelogging. In *Proceedings of the 30th International BCS Human Computer Interaction Conference: Companion Volume*, page 15. BCS Learning & Development Ltd., 2016.

[18] L. Chung and J. C. S. do Prado Leite. On non-functional requirements in software engineering. In *Conceptual modeling: Foundations and applications*, pages 363–379. Springer, 2009.

[19] K. P. Coopamootoo and T. Groß. Why privacy is all but forgotten. *Proceedings on Privacy Enhancing Technologies*, 2017(4):97–118, 2017.

[20] C. L. Corritore, B. Kracher, and S. Wiedenbeck. On-line trust: concepts, evolving themes, a model. *International journal of human-computer studies*, 58(6):737–758, 2003.

[21] E. Courcier, R. Thomson, D. Mellor, and P. Yam. An epidemiological study of environmental factors associated with canine obesity. *Journal of Small Animal Practice*, 51(7): 362–367, 2010.

[22] Credence Research. Pet Wearables Market By Technology (GPS, RFID, Sensors), By Product (Smart Tags, Smart Collars, Smart Vests) - Growth, Future Prospects, And Competitive Analysis, 2017–2025. http://www.credenceresearch.com/report/pet-wearables-market, 2017. Online; accessed 11 December 2018.

[23] T. Denning, Z. Dehlawi, and T. Kohno. In situ with bystanders of augmented reality glasses: Perspectives on recording and privacy-mediating technologies. In *Proceedings of the 32nd annual ACM conference on Human factors in computing systems*, pages 2377–2386. ACM, 2014.

[24] L. Festinger. *A theory of cognitive dissonance*, volume 2. Stanford university press, 1957.

[25] C. Gabrielatos. Keyness analysis: nature, metrics and techniques. *Corpus Approaches to Discourse: A Critical Review*, pages 225–258, 2018.

[26] Get Wüf. Get Wüf. http://www.getwuf.com, 2019. Online; expired domain; accessed 11 June 2019.

[27] M. Gruteser and X. Liu. Protecting privacy in continuous location-tracking applications. *IEEE Security & Privacy*, (2): 28–34, 2004.

[28] J. M. Haney and W. G. Lutters. "it's scary... it's confusing... it's dull": How cybersecurity advocates overcome negative perceptions of security. In *Fourteenth Symposium on Usable Privacy and Security ({SOUPS} 2018)*, pages 411–425, 2018.

[29] A. Hardie. Log ratio–an informal introduction. *Retrieved from http://cass.lancs.ac.uk*, 2014.

[30] L. M. Hines. Historical perspectives on the human-animal bond. *American Behavioral Scientist*, 47(1):7–15, 2003.

[31] R. Hoyle, R. Templeman, S. Armes, D. Anthony, D. Crandall, and A. Kapadia. Privacy behaviors of lifeloggers using wearable cameras. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, pages 571–582. ACM, 2014.

[32] S. Hughes and D. Cohen. Can online consumers contribute to drug knowledge? a mixed-methods comparison of consumer-generated and professionally controlled psychotropic medication information on the internet. *Journal of medical Internet research*, 13(3), 2011.

[33] C. J. Hutto and E. Gilbert. Vader: A parsimonious rule-based model for sentiment analysis of social media text. In *Eighth International Conference on Weblogs and Social Media (ICWSM-14)*, 2014.

[34] L. Jack and Y. Tsai. Using text mining of amazon reviews to explore user-defined product highlights and issues. In *Proceedings of the International Conference on Data Mining (DMIN)*, page 92. The Steering Committee of The World Congress in Computer Science, Computer . . . , 2015.

[35] Juarawee Kittisilpa / Reuters. 'Smart vest' turns stray dogs into Thailand's street guardians . https://www.reuters.com/article/us-thailand-watchdogs/smart-vest-turns-stray-dogs-into-thailands-street-guardians-idUSKCN1BC58J, 2019. Online; accessed 11 June 2019.

[36] R. Kang, L. Dabbish, N. Fruchter, and S. Kiesler. "my data just goes everywhere:" user mental models of the internet and implications for privacy and security. In *Symposium on Usable Privacy and Security (SOUPS)*, pages 39–52. USENIX Association Berkeley, CA, 2015.

[37] H. Krasnova, T. Hildebrand, and O. Guenther. Investigating the value of privacy on online social networks: conjoint analysis. In *Proceedings of the International Conference on Information Systems (ICIS)*, 2009.

[38] L. Lee, J. Lee, S. Egelman, and D. Wagner. Information disclosure concerns in the age of wearable computing. In *Proceedings of the 2016 Workshop on Usable Security*, 2016.

[39] M. Lee and M. R. Lee. Beyond the wearable hype. *IT Professional*, (5):59–61, 2015.

[40] D. Leibenger, F. Möllers, A. Petrlic, R. Petrlic, and C. Sorge. Privacy challenges in the quantified self movement–an eu perspective. *Proceedings on Privacy Enhancing Technologies*, 2016(4):315–334, 2016.

[41] A. Melander-Wikman, Y. Fältholm, and G. Gard. Safety vs. privacy: elderly persons' experiences of a mobile safety alarm. *Health & social care in the community*, 16(4):337–346, 2008.

[42] R. Moll, S. Pieschl, and R. Bromme. Trust into collective privacy? the role of subjective theories for self-disclosure in online communication. *Societies*, 4(4):770–784, 2014.

[43] A. D. Moore. Privacy: Its meaning and value. *American Philosophical Quarterly*, 40(3):215–227, 2003.

[44] C. Morley and J. Fook. The importance of pet loss and some implications for services. *Mortality*, 10(2):127–143, 2005.

[45] V. G. Motti and K. Caine. Users' privacy concerns about wearables. In *International Conference on Financial Cryptography and Data Security*, pages 231–244. Springer, 2015.

[46] Mozilla Foundation. *privacy not included. https://foundation.mozilla.org/en/privacynotincluded/categories/Pets/, 2019. Online; accessed 11 June 2019.

[47] S. M. Mudambi and D. Schuff. Research note: What makes a helpful online review? a study of customer reviews on amazon. com. *MIS quarterly*, pages 185–200, 2010.

[48] A. Mukherjee, V. Venkataraman, B. Liu, and N. Glance. Fake review detection: Classification and analysis of real and pseudo reviews. *UIC-CS-03-2013. Technical Report*, 2013.

[49] P. E. Naeini, S. Bhagavatula, H. Habib, M. Degeling, L. Bauer, L. Cranor, and N. Sadeh. Privacy expectations and preferences in an iot world. In *Proceedings of the 13th Symposium on Usable Privacy and Security (SOUPS)*, 2017.

[50] M. K. Nelson. Watching children: Describing the use of baby monitors on epinions. com. *Journal of Family Issues*, 29(4):516–538, 2008.

[51] M. L. Nijland, F. Stam, and J. C. Seidell. Overweight in dogs, but not in cats, is related to overweight in their owners. *Public health nutrition*, 13(1):102–106, 2010.

[52] PetCommunity. petcommunity. https://petcommunity.com/, 2019. Online; accessed 11 June 2019.

[53] M. F. Porter. An algorithm for suffix stripping. *Program*, 14 (3):130–137, 1980.

[54] Y. Pu and J. Grossklags. Towards a model on the factors influencing social app users' valuation of interdependent privacy. *Proceedings on privacy enhancing technologies*, 2016(2):61–81, 2016.

[55] E. Rader and J. Slaker. The importance of visibility for folk theories of sensor data. In *Symposium on Usable Privacy and Security (SOUPS)*, 2017.

[56] Y. Rashidi, T. Ahmed, F. Patel, E. Fath, A. Kapadia, C. Nippert-Eng, and N. M. Su. " you don't want to be the next meme": College students' workarounds to manage privacy in the era of pervasive photography. In *Fourteenth Symposium on Usable Privacy and Security ({SOUPS} 2018)*, pages 143–157, 2018.

[57] P. Rayson and R. Garside. Comparing corpora using frequency profiling. In *Proceedings of the Workshop on Comparing Corpora Volume 9*, pages 1–6. Association for Computational Linguistics, 2000.

[58] P. M. Regan, G. FitzGerald, and P. Balint. Generational views of information privacy? *Innovation: The European Journal of Social Science Research*, 26(1-2):81–99, 2013.

[59] B. Schneier. The eternal value of privacy, 2016. URL https://www.schneier.com/essays/archives/2006/05/the_eternal_value_of.html.

[60] S. Seneviratne, Y. Hu, T. Nguyen, G. Lan, S. Khalifa, K. Thilakarathna, M. Hassan, and A. Seneviratne. A survey of wearable devices and challenges. *IEEE Communications Surveys & Tutorials*, 19(4):2573–2620, 2017.

[61] D. J. Solove. I've got nothing to hide and other misunderstandings of privacy. *San Diego L. Rev.*, 44:745, 2007.

[62] C. Spensky, J. Stewart, A. Yerukhimovich, R. Shay, A. Trachtenberg, R. Housley, and R. K. Cunningham. Sok: Privacy on mobile devices–it's complicated. *Proceedings on Privacy Enhancing Technologies*, 2016(3):96–116, 2016.

[63] K. Spiller, K. Ball, A. Bandara, M. Meadows, C. McCormick, B. Nuseibeh, and B. A. Price. Data privacy: Users' thoughts on quantified self personal data. In *Self-Tracking*, pages 111–124. Springer, 2018.

[64] H. J. Spiro. Privacy in comparative perspective. In *Privacy and Personality*, pages 121–148. Routledge, 2017.

[65] M. Trenz and B. Berger. Analyzing online customer reviews-an interdisciplinary literature review and research agenda. In *ECIS*, page 83, 2013.

[66] L. Tzivian, M. Friger, and T. Kushnir. Associations between stress and quality of life: Differences between owners keeping a living dog or losing a dog by euthanasia. *PloS One*, 10(3): e0121081, 2015.

[67] R. Unuchek and R. Sako. I know where your pet is. Blog May 22, 2018.

[68] D. van der Linden et al. Buddy's wearable is not your buddy: privacy implications of pet wearables. *IEEE Secu-*

rity and Privacy, 17(3), 2018.

[69] J. van Heek, K. Aming, and M. Ziefle. "how fear of crime affects needs for privacy & safety": Acceptance of surveillance technologies in smart cities. In *2016 5th International Conference on Smart Cities and Green ICT Systems (SMARTGREENS)*, pages 1–12. IEEE, 2016.

[70] Y. Wang, H. Xia, Y. Yao, and Y. Huang. Flying eyes and hidden controllers: A qualitative study of people's privacy perceptions of civilian drones in the us. *Proceedings on Privacy Enhancing Technologies*, 2016(3):172–190, 2016.

[71] Y. D. Wang and H. H. Emurian. An overview of online trust: Concepts, elements, and implications. *Computers in human behavior*, 21(1):105–125, 2005.

[72] M. Winkler, A. S. Abrahams, R. Gruss, and J. P. Ehsani. Toy safety surveillance from online reviews. *Decision support systems*, 90:23–32, 2016.

[73] Z. Yang and X. Fang. Online service quality dimensions and their relationships with satisfaction: A content analysis of customer reviews of securities brokerage services. *Int. J. Service Industry Management*, 15(3):302–326, 2004.

[74] Z. Yang, M. Jun, and R. T. Peterson. Measuring customer perceived online service quality: scale development and managerial implications. *International Journal of Operations & Production Management*, 24(11):1149–1174, 2004.

[75] Zamansky et al. Log my dog – perceived impact of canine activity tracking. *IEEE Computer*, 2018. major revisions.

[76] A. Zamansky and D. van der Linden. Activity trackers for raising guide dogs: Challenges and opportunities. *IEEE Technology and Society Magazine*, 37(4):62–69, 2018.

[77] S. D. Zansberg and J. K. Fischer. Privacy expectations in online social media-an emerging generational divide. *Comm. Law.*, 28:1, 2011.

[78] E. Zeng, S. Mare, and F. Roesner. End user security & privacy concerns with smart homes. In *Symposium on Usable Privacy and Security (SOUPS)*, 2017.

A Pet owner questionnaire

- Participant information sheet and informed consent.
  ○I consent to begin the study
- Pet wearables are devices that your pet wears on their collar which can do a range of things: help you keep your pet healthy & happy, make pet ownership easier, help you have more fun with your pet, or help you find your pet.
  Have you heard of pet wearables before?
  ○No
  ○Yes – I have heard of them
  ○Yes – I have used a pet wearable
- *If they have used a pet wearable:*
  - What would be the main reason for you to ***no longer*** use your pet wearable, if any? (select all that apply)
    ☐I no longer see a use for it
    ☐The battery doesn't last long enough
    ☐I don't feel it is accurate enough
    ☐I am concerned for my pet's welfare/health
    ☐I am concerned for my privacy
    ☐My pet breaks it too easily
    ☐Other (please specify): ☐
  - Can you elaborate on the reason(s) you selected for *no longer* using a pet wearable?
    ☐
- *If they have not used a pet wearable:*
  - What would be the main reason for you to ***not*** purchase a pet wearable, if any? (select all that apply)
    ☐I see no use for it
    ☐I don't think the battery will last very long
    ☐I wouldn't trust it to be accurate
    ☐It's too expensive
    ☐I would be concerned for my pet's welfare/health
    ☐I would be concerned for my privacy
    ☐I think my pet would break it
    ☐Other (please specify): ☐
  - Can you elaborate on the reason(s) you selected for *no longer* using a pet wearable?
    ☐

B Thematic analysis codebook

B.1 Privacy concern is trumped by another factor

Major theme definition: Review indicates some concerns other than privacy that are most salient, in a context where the owner's privacy is potentially impacted.

B.1.1 Functionality trumps privacy

Definition: Review indicates (desired) functionality of the pet wearable is seen as more beneficial than other concerns.

Example Quote(s): "Another cool thing about the app is storing medical records. Since we are new to town I have to re-enroll her in a daycare, dog parks,etc. and I'm so glad I don't have to cart all those papers around with me. I already have enough in my purse!" (P468)

B.1.2 Emotional attachment trumps privacy

Definition: Review indicates the pet wearable mediates in the emotional bond between owner and pet, seen as more beneficial than other concerns.

Example Quote(s): "we thought we had lost our dog. My wife was crying and I was at my wits ends. [...] We could not live through that feeling again, sowe found Tagg Tracker." (P5357)

B.1.3 Consumers do not make the leap

Definition: Review indicates a potential privacy concern is raised, but not explicitly pointed out as such.

Example Quote(s): "So, apparently your device isn't picking up just one other dog, but apparently any dog that happens to have their device turned on at the same time as mine." (P135)

B.1.4 Generational differences in privacy expectations

Definition: Review raises a privacy concern and explains why 'others' do not hold similar views.

Example Quote(s): "I think it's just too damn fancy and wasn't designed for real people or dogs but designed by some 20 y/o tech wizards that want access to your phone data and location 24/7 so they can spam you advertisements. Time will tell but that's my gut feeling." (P711)

B.2 Bystander privacy concern is trumped by another factor.

Major theme definition: Review indicates some concerns other than privacy that are most salient, in a context where bystanders ' privacy is potentially impacted.

B.2.1 We want to keep an eye on those interacting with our pets

Definition: Review indicates that observation of bystanders enables more responsible care of their pets.

Example Quote(s): "[. . .] So it's nice to have the peace of mind that nobody is cheating your furry friend on their much needed playtime." (P2689)

B.2.2 Functionality trumps privacy

Definition: Review indicates (desired) functionality of the pet wearable is seen as more beneficial than other concerns.

Example Quote(s): "could they make a 'Go Pro' camera that also attaches so that we could get a video of where she has been and what she has been up to? I'm sure that will be coming in the next version :)" (P6898)

B.3 Pet wearables are worn by humans.

Major theme definition: Review indicates the pet wearable is used for a different purpose than originally intended: a human user.

B.3.1 Pet wearables work well for the cognitively impaired

Definition: Review indicates the pet wearable's suitability for use with cognitively impaired human individuals.

Example Quote(s): "I will also add that this tracker actually worked better for keeping an eye on my mother than the much more expensive 'dementia tracker' I also bought at the same time." (P2128)

B.3.2 Pet wearables work well for kids

Definition: Review indicates the pet wearable's suitability for use with children.

Example Quote(s): "So we don't actually have this attached to a pet – we put it on a belt for our 6-yr old son to give him the freedom to go outside and play with his friends like it's 1988." (P3452)

C Figures & tables

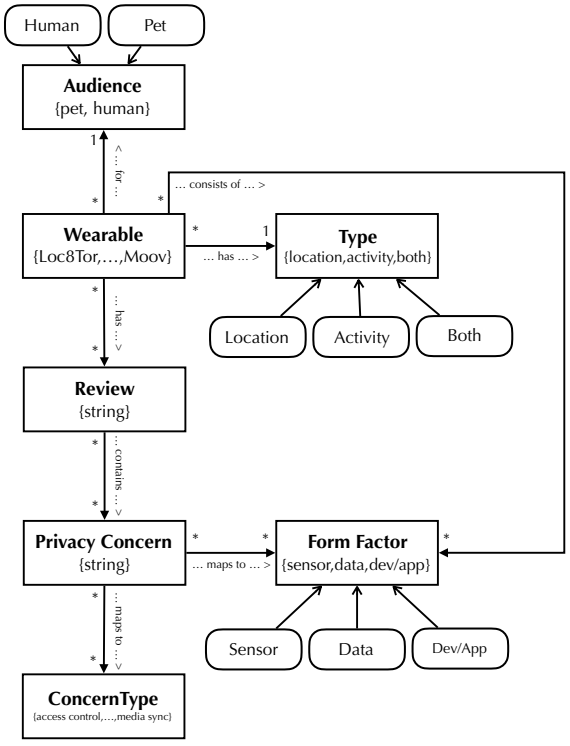

Fig. 1. Model of the research objects.

Table 5. Reviews matching a keyword, with final accumulation at a threshold of 2 distinct keyword matches per review

keyword	pet hits	%	human hits	%	ratio
cumulative	962	11.97	1299	6.36	1.88
scared	75	0.93	15	0.07	12.71
fear	64	0.80	18	0.09	9.04
location	1684	20.95	538	2.63	7.96
preserve	8	0.10	4	0.02	5.08
critical	43	0.53	26	0.13	4.20
concern	204	2.54	135	0.66	3.84
		...			
invasion	1	0.01	7	0.03	0.36
suspicious	5	0.06	38	0.19	0.33
synchronize	5	0.06	42	0.21	0.30
twitter	1	0.01	9	0.04	0.28
third party	4	0.05	39	0.19	0.26
discreet	3	0.04	43	0.21	0.18

Table 6. Pet wearables with significantly more positive or negative reviews than average (judged by star rating [★] and sentiment), their number of known vulnerabilities, and whether privacy policies cover the data captured by devices (✓) or omit information (**?**).

Device	Opinion	★	Sent	Vulns	Policy
Whistle 3	+	✓	✓	4	✓
FitBark	+	✓	✓		✓
TractiveGPS	-	✓	✓	1	**?**
TractiveMotion	-	✓	✓		**?**
Access 88	-	✓	✓		
TabCat	-	✓	✓		**?**
Tagg	-	✓	✓		
Link AKC	-	✓		1	**?**
DOTT	-	✓			

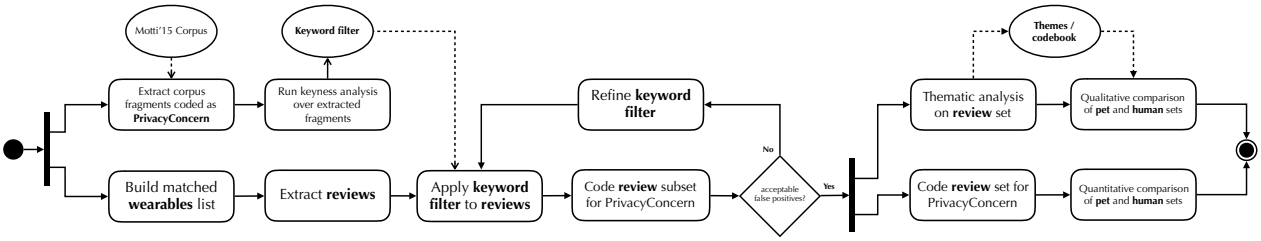

Fig. 2. Activity diagram of the study.